JUNIPER NETWORKS | Engineering Simplicity

vSRX Deployment Guide for Google Cloud Platform

Published
2020-12-28

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

vSRX Deployment Guide for Google Cloud Platform

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at https://support.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About This Guide

Use this guide to install the vSRX Virtual Firewall in a Google virtual private cloud (VPC). This guide also includes basic vSRX configuration and management procedures.

After completing the installation and basic configuration procedures covered in this guide, refer to the Junos OS documentation for information about further software configuration.

1

CHAPTER

Overview

vSRX Overview

SUMMARY

In this topic you learn about vSRX architecture and its benefits.

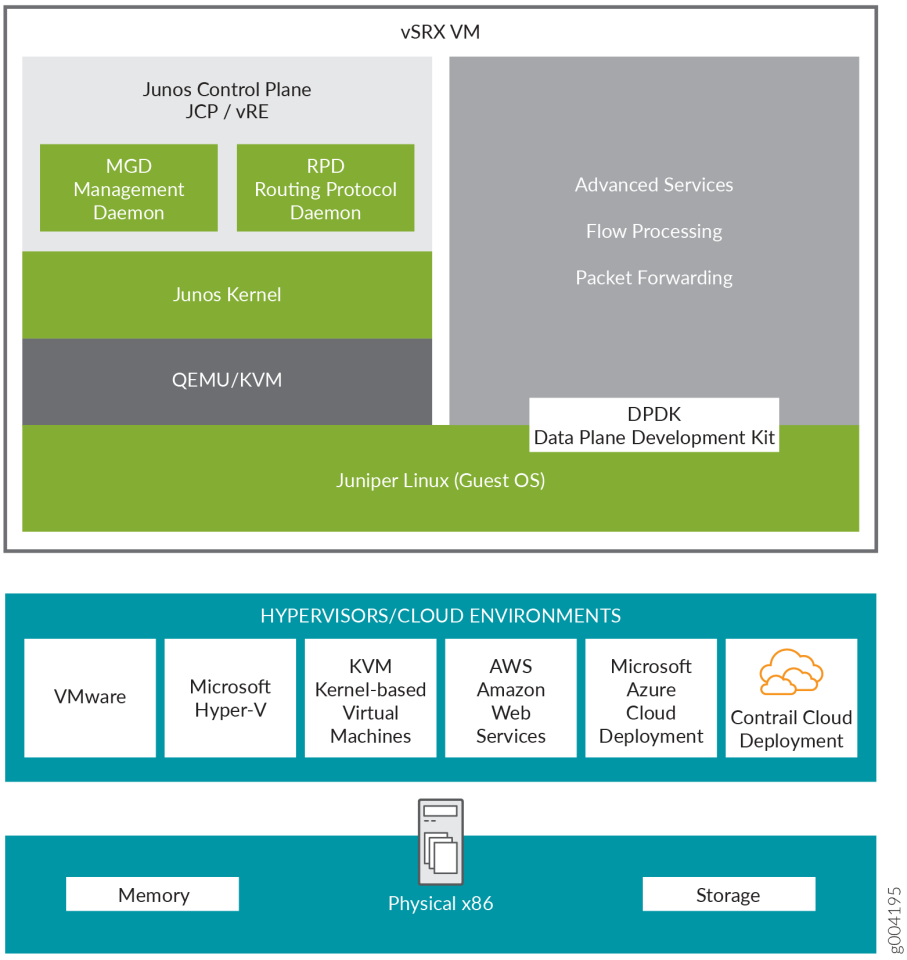
IN THIS SECTION

vSRX is a virtual security appliance that provides security and networking services at the perimeter or edge in virtualized private or public *cloud* environments. vSRX runs as a virtual machine (*VM*) on a standard x86 server. vSRX is built on the Junos operating system (Junos OS) and delivers networking and security features similar to those available on the software releases for the SRX Series Services Gateways.

The vSRX provides you with a complete Next-Generation Firewall (NGFW) solution, including core firewall, VPN, NAT, advanced Layer 4 through Layer 7 security services such as Application Security, intrusion detection and prevention (IPS), and UTM features including Enhanced Web Filtering and Anti-Virus. Combined with Sky ATP, the vSRX offers a cloud-based advanced anti-malware service with dynamic analysis to protect against sophisticated malware, and provides built-in machine learning to improve verdict efficacy and decrease time to remediation.

Figure 1 on page 3 shows the high-level architecture.

Figure 1: vSRX Architecture



vSRX includes the Junos control plane (JCP) and the packet forwarding engine (PFE) components that make up the data plane. vSRX uses one virtual CPU (vCPU) for the JCP and at least one vCPU for the PFE. Starting in Junos OS Release 15.1X49-D70 and Junos OS Release 17.3R1, multi-core vSRX supports scaling vCPUs and virtual RAM (vRAM). Additional vCPUs are applied to the data plane to increase performance.

Junos OS Release 18.4R1 supports a new software architecture vSRX 3.0 that removes dual OS and nested virtualization requirement of existing vSRX architecture.

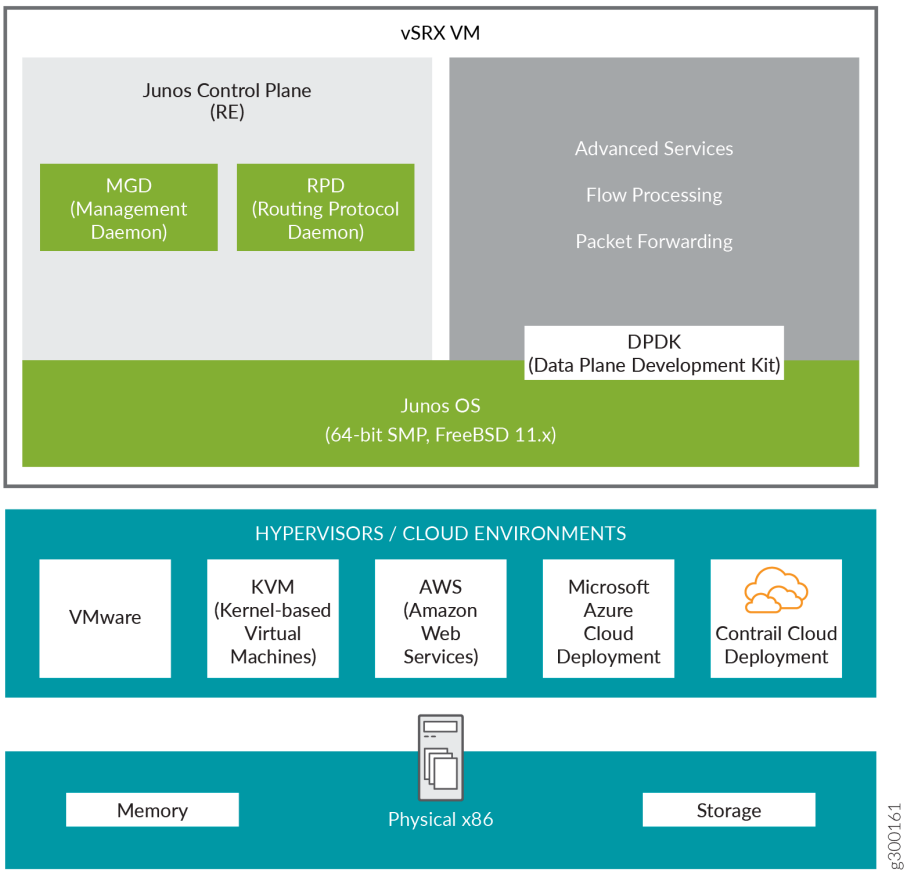
In vSRX 3.0 architecture, FreeBSD 11.x is used as the guest OS and the Routing Engine and Packet Forwarding Engine runs on FreeBSD 11.x as single virtual machine for improved performance and scalability. vSRX 3.0 uses DPDK to process the data packets in the data plane. A direct Junos upgrade from vSRX to vSRX 3.0 software is not supported.

vSRX 3.0 has the following enhancements compared to vSRX:

- Removed the restriction of requiring nested VM support in hypervisors.
- Removed the restriction of requiring ports connected to control plane to have Promiscuous mode enabled.
- Improved boot time and enhanced responsiveness of the control plane during management operations.
- Improved live migration.

Figure 2 on page 4 shows the high-level architecture for vSRX 3.0

Figure 2: vSRX 3.0 Architecture



Benefits

vSRX on standard x86 servers enables you to quickly introduce new services, deliver customized services to customers, and scale security services based on dynamic needs. vSRX is ideal for public, private, and hybrid cloud environments.

Some of the key benefits of vSRX in a virtualized private or public cloud multitenant environment include:

- *Stateful firewall* protection at the tenant edge
- Faster deployment of virtual firewalls into new sites
- Ability to run on top of various hypervisors and public cloud infrastructures
- Full routing, *VPN*, core security, and networking capabilities
- Application security features (including IPS and App-Secure)
- Content security features (including Anti Virus, Web Filtering, Anti Spam, and Content Filtering)
- Centralized management with Junos Space Security Director and local management with J-Web Interface
- Juniper Networks Sky Advanced Threat Prevention (Sky ATP) integration

Release History Table

Release	Description
15.1X49-D70	Starting in Junos OS Release 15.1X49-D70 and Junos OS Release 17.3R1, multi-core vSRX supports scaling vCPUs and virtual RAM (vRAM). Additional vCPUs are applied to the data plane to increase performance.

Understand vSRX Deployment with Google Cloud

IN THIS SECTION

Understand vSRX Deployment with Google Cloud Platform

IN THIS SECTION

Google Cloud Platform (GCP) is a public cloud service provided by Google. Like Amazon Web Service (AWS) and Microsoft Azure, GCP offers a suite of products and services that allow you to build and host applications and websites, store data, and analyze data on Google's scalable infrastructure. A pay-as-you-go model is delivered and saves you from building your own private cloud using dedicated hardware.

Google's virtual private cloud (VPC) gives you the flexibility to scale and control how workloads connect regionally and globally. When you connect your on-premises or remote resources to GCP, you will have global access to your VPCs without needing to replicate connectivity or administrative policies in each region.

vSRX in a public cloud can be used for protecting service VMs from public Internet or protecting VMs in different subnets, or used as VPN Gateways.

Like AWS, GCP allows you to build your own VPCs on top of Google's public infrastructure. Unlike AWS, GCP uses KVM instead of modified Xen as the hypervisor for VM management.

In a Google cloud, vSRX instances run on top of Google VPCs. A Google VPC has the following properties:

- Provides a global private communication space.
- Supports multitenancy in an organization.
- Provides private communication between Google Cloud Platform (GCP) resources, such as Computing Engine and Cloud Storage.
- Provides security for configuration access using identify and access management (IAM).
- Extensible across hybrid environments.

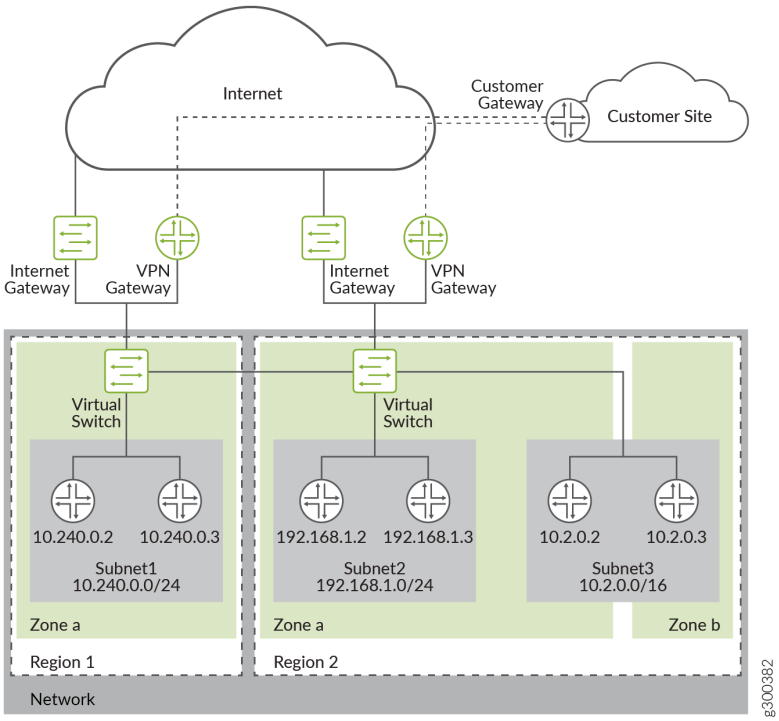
When you create a resource in GCP, you choose a network and subnet. For resources other than instance templates, you also select a zone or a region. Selecting a zone implicitly selects its parent region. Because subnets are regional objects, the region you select for a resource determines the subnets it can use.

The process of creating an instance involves selecting a zone, a network, and a subnet. The subnets available for selection are restricted to those in the selected region. GCP assigns the instance an IP address from the range of available addresses in the subnet.

The process of creating a managed instance group involves selecting a zone or region, depending on the group type, and an instance template. The instance templates available for selection are restricted to those whose defined subnets are in the same region selected for the managed instance group. Instance templates are global resources. The process of creating an instance template involves selecting a network and a subnet. If you select an auto-mode network, you can choose “auto subnet” to defer subnet selection to one that is available in the selected region of any managed instance group that would use the template, because auto-mode networks have a subnet in every region by definition.

An example of a typical Google VPC is shown in Figure 3 on page 7.

Figure 3: Example of a Google VPC



The vSRX instance is launched with multiple virtual interfaces in VPC subnets. The first interface (fxp0) will be the management interface. It is connected to the Internet gateway for public access. You can use SSH to access the interface and manage the virtual device with Junos CLI, just as you can with SRX Series devices. The subsequent interfaces are revenue ports. They are managed by the flowd process running on Linux and handle all the traffic. On GCP, a maximum of 8 network interfaces are allowed per vSRX instance.

Some of the initial provisioning parameters for first boot are host name, root password, SSH public key, management interface (fxp0) IP address, and default gateway IP address.

Starting in Junos OS Release 19.2R1, vSRX instances with 2 vCPUs, 4-GB memory, and 19-GB disk space are supported on GCP.

Manage Access to Instances

To create and manage instances, you can use a variety of tools, including the Google Cloud Platform Console, the gcloud command-line tool, and the REST API. To configure applications on your instances, connect to the instance using SSH for Linux instances.

You can manage access to your instances using one of the following methods:

- **Linux instance:**
  - Manage instance access using OS login, which allows you to associate SSH keys with your Google account or G Suite account and manage administrator or non-administrator access to instances through identity and access management (IAM) roles. If you connect to your instances using the gcloud command-line tool or SSH from the console, Compute Engine can automatically generate SSH keys for you and apply them to your Google account or G Suite account.
  - Manage your SSH keys in project or instance metadata, which grants administrator access to instances with metadata access that do not use OS Login. If you connect to your instances using the gcloud command-line tool or SSH from the console, Compute Engine can automatically generate SSH keys for you and apply them to project metadata.
- **Windows Server instances**—Create a password for a Windows Server instance.

Access Instances

After you configure access to your instances, you can connect to your instances using one of several options. For more information about connecting your instances, see Connecting to instances.

Requirements for vSRX on Google Cloud Platform

IN THIS SECTION

Google Compute Engine Instance Types

To create a vSRX instance, you need to choose a machine type. The machine type specifies a particular collection of virtualized hardware resources available to a VM instance, including the memory size, vCPU count, and maximum disk capacity.

Google Compute Engine allows you to use predefined machine or instances types or customized machine or instance types based on your needs. Table 1 on page 9 below shows the predefined machine types available in Google Compute Engine.

Table 1: Google Compute Engine Instance Types

Machine Name	Description	vCPUs	Memory (GB)	vSRX 3.0 Instance	Maximum number of Persistent Disks	Maximum total Persistent Disk Size (TB)	RSS Type
n1-standard-2	Standard machine type with 2 vCPUs and 7.5 GB of memory	2	7.50	VSRX-2CPU-7G memory	16	64	HWRSS
n1-standard-4	Standard machine type with 4 vCPUs and 15 GB of memory	4	15	VSRX-4CPU-15G memory	16	64	SWRSS

Table 1: Google Compute Engine Instance Types *(Continued)*

Machine Name	Description	vCPUs	Memory (GB)	vSRX 3.0 Instance	Maximum number of Persistent Disks	Maximum total Persistent Disk Size (TB)	RSS Type
n1-standard-8	Standard machine type with 8 vCPUs and 30 GB of memory	8	30	VSRX-8CPU-30G memory	16	64	SWRSS
n1-standard-16	Standard machine type with 16 vCPUs and 60 GB of memory	16	60	VSRX-16CPU-60G memory	16	64	SWRSS

A single Google Compute Engine instance supports up to eight network interfaces. If you want to configure eight interfaces, choose n1-standard-8 or a larger machine type. After choosing the machine type, define the networking attributes and SSH Keys for the VM. For more information on network interfaces, see Creating instances with multiple network interfaces.

vSRX Support for Google Cloud

Starting in Junos OS Release 19.2R1, vSRX with 1 Junos Control Plane (JCP) vCPU, 1 data plane vCPU, and 4 GB of vRAM is supported.

vSRX Specifications for GCP

IN THIS SECTION

This topic provides details about hardware and software requirements for deploying vSRX with Google.

Minimum System Requirements for Google Cloud Platform

Table 2 on page 11 lists the minimum system requirements and the Junos OS release in which a particular software specification was introduced for vSRX instances to be deployed on GCP.

Table 2: Minimum System Requirements for vSRX on GCP

Component	Specification	Release Introduced
Memory	4 GB	Junos OS Release 19.2R1
Disk space	19-GB IDE drive	Junos OS Release 19.2R1
vCPUs	1 Junos Control Plane (JCP) vCPU and 1 data plane vCPU	Junos OS Release 19.2R1
vNICs	2-8 vNICs • Virtio • SR-IOV is not supported by GCP.	Junos OS Release 19.2R1
Software feature license	For more information, see Flex Software Subscription Model and Juniper Flex Program Support for Juniper Products.	NA

Table 2: Minimum System Requirements for vSRX on GCP *(Continued)*

Component	Specification	Release Introduced
Software packaging	Google Compute Engine has specific requirements for the bootable image that is imported to Google cloud space. For more information, see https://cloud.google.com/compute/docs/images/import-existing-image#create_image_file. For initial deployment, the .img file is used and for software upgrade, the .tgz image is used.	NA

Interface Mapping for vSRX on Google Cloud

Each network adapter defined for a vSRX is mapped to a specific interface, depending on whether the vSRX instance is a standalone VM or one of a cluster pair for high availability. The interface names and mappings in vSRX are shown in Table 3 on page 12.

Note the following:

- In standalone mode:
  - fxp0 is the out-of-band management interface.
  - ge-0/0/0 is the first traffic (revenue) interface.

Table 3 on page 12 shows the interface names and mappings for a standalone vSRX on Google cloud.

Table 3: Interface Names for a Standalone vSRX on GCP

Network Adapter	Interface Name in Junos OS for vSRX
1	fxp0

Table 3: Interface Names for a Standalone vSRX on GCP *(Continued)*

Network Adapter	Interface Name in Junos OS for vSRX
2	ge-0/0/0
3	ge-0/0/1
4	ge-0/0/2
5	ge-0/0/3
6	ge-0/0/4
7	ge-0/0/5
8	ge-0/0/6

vSRX Default Settings on GCP

vSRX requires the following basic configuration settings:

- Interfaces must be assigned IP addresses.
- Interfaces must be bound to zones.
- Policies must be configured between zones to permit or deny traffic.

Table 4 on page 13 lists the factory-default settings for security policies on the vSRX instance.

Table 4: Factory-Default Settings for Security Policies

Source Zone	Destination Zone	Policy Action
trust	untrust	permit

Table 4: Factory-Default Settings for Security Policies *(Continued)*

Source Zone	Destination Zone	Policy Action
trust	trust	permit
untrust	trust	deny

Junos OS Features Supported on vSRX

SUMMARY

This topic provides details of the Junos OS features supported and not supported on vSRX.

IN THIS SECTION

SRX Series Features Supported on vSRX

vSRX inherits most of the branch SRX Series features with the following considerations shown in Table 5 on page 15.

To determine the Junos OS features supported on vSRX, use the Juniper Networks Feature Explorer, a Web-based application that helps you to explore and compare Junos OS feature information to find the right software release and hardware platform for your network. Find Feature Explorer at: Feature Explorer: vSRX .

Table 5: vSRX Feature Considerations

Feature	Description	
IDP	The IDP feature is subscription based and must be purchased. After purchase, you can activate the IDP feature with the license key. For SRX Series IDP configuration details, see: Understanding Intrusion Detection and Prevention for SRX Series	
IPSec VPNs	Starting in Junos OS Release 19.3R1, vSRX supports the following authentication algorithms and encryption algorithms: • Authentication algorithm: hmac-sha1-96 and HMAC-SHA-256-128 authentication • Encryption algorithm: aes-128-cbc Starting in Junos OS Release 20.3R1, vSRX supports 10,000 IPsec VPN tunnels. To support the increased number of IPsec VPN tunnels, a minimum of 19 vCPUs are required. Out of the 19 vCPUs, 3 vCPUs must be dedicated to RE. You must run the **request system software add optional://junos-ike.tgz** command the first time you wish to enable increased IPsec tunnel capacity. For subsequent software upgrades of the instance, the junos-ike package is upgraded automatically from the new Junos OS releases installed in the instance. If chassis cluster is enabled then run this command on both the nodes. You can configure the number of vCPUs allocated to Junos Routing Engine using the **set security forwarding-options resource-manager cpu re <value>**. **NOTE**: 64 G memory is required to support 10000 tunnels in PMI mode. [See show security ipsec security-associations, show security ike tunnel-map, and show security ipsec tunnel-distribution.]	
IPsec VPN - Tunnel Scaling on vSRX	Types of Tunnels	Number of tunnels supported
	Site-Site VPN tunnels	2000

Table 5: vSRX Feature Considerations *(Continued)*

Feature	Description	
	AutoVPN tunnels	10,000
	IKE SA (Site-to-site)	2000
	IKE SA (AutoVPN)	10,000
	IKE SA (Site-to-site + AutoVPN)	10,000
	IPSec SA pairs (Site-to-site)	10,000 With 2000 IKE SAs, we can have 10,000 IPSec SA.
	IPSec SA pairs (AutoVPN)	10,000
	Site-to-site + AutoVPN IPSec SA pairs	2000 Site-to-site 8000 AutoVPN
	Site-to-site + AutoVPN tunnels	2000 Site-to-site 8000 AutoVPN
ISSU	ISSU is not supported.	
Logical Systems	Starting in Junos OS Release 20.1R1, you can configure logical systems and tenant systems on vSRX and vSRX 3.0 instances. With Junos OS, you can partition a single security device into multiple logical devices that can perform independent tasks. Each logical system has its own discrete administrative domain, logical interfaces, routing instances, security firewall and other security features. See Logical Systems Overview.	

Table 5: vSRX Feature Considerations *(Continued)*

Feature	Description
PowerMode IPsec	Starting in Junos OS Release 20.1R1, vSRX 3.0 instances support PowerMode IPsec that provides IPsec performance improvements using Vector Packet Processing (VPP) and Intel AES-NI instructions. PowerMode IPsec is a small software block inside the SRX PFE (SRX Packet Forwarding Engine) that is activated when PowerMode is enabled. Supported Features in PowerMode IPsec • IPsec functionality • Traffic selectors • Secure tunnel interface (st0) • All control plane IKE functionality • Auto VPN with traffic selector • Auto VPN with routing protocol • IPv6 • Stateful Layer 4 firewall • High-Availability • NAT-T Non-Supported Features in PowerMode IPsec • NAT • IPsec in IPsec • GTP/SCTP firewall • Application firewall/AppSecure • QoS • Nested tunnel • Screen

Table 5: vSRX Feature Considerations *(Continued)*

Feature	Description
	• Multicast • Host traffic
Tenant Systems	Starting in Junos OS Release 20.1R1, you can configure tenant systems on vSRX and vSRX 3.0 instances. A tenant system provides logical partitioning of the SRX device into multiple domains similar to logical systems and provides high scalability. See Tenant Systems Overview.
Transparent mode	The known behaviors for transparent mode support on vSRX are: • The default MAC learning table size is restricted to 16,383 entries. For information about configuring transparent mode for vSRX, see Layer 2 Bridging and Transparent Mode Overview.

Table 5: vSRX Feature Considerations *(Continued)*

Feature	Description
UTM	• The UTM feature is subscription based and must be purchased. After purchase, you can activate the UTM feature with the license key. • Starting in Junos OS Release 19.4R1, vSRX 3.0 instances support the Avira scan engine, which is an on-device antivirus scanning engine. See On-Device Antivirus Scan Engine. • For SRX Series UTM configuration details, see Unified Threat Management Overview. • For SRX Series UTM antispam configuration details, see Antispam Filtering Overview. • **Advanced resource management (vSRX 3.0)**—Starting in Junos OS Release 19.4R1, vSRX 3.0 manages the additional system resource requirements for UTM-and IDP-specific services by reallocating CPU cores and extra memory. These values for memory and CPU cores are not user configured. Previously, system resources such as memory and CPU cores were fixed. You can view the allocated CPU and memory for advance security services on vSRX 3.0 instance by using the **show security forward-options resource-manager settings** command. To view the flow session scaling, use the **show security monitoring** command. [See show security monitoring and show security forward-options resource-manager settings.]

Some Junos OS software features require a license to activate the feature. To understand more about vSRX Licenses, see, Licenses for vSRX. Please refer to the Licensing Guide for general information about License Management. Please refer to the product Data Sheets for further details, or contact your Juniper Account Team or Juniper Partner.

SRX Series Features Not Supported on vSRX

vSRX inherits many features from the SRX Series device product line. Table 6 on page 20 lists SRX Series features that are not applicable in a virtualized environment, that are not currently supported, or that have qualified support on vSRX.

Table 6: SRX Series Features Not Supported on vSRX

SRX Series Feature	vSRX Notes
Application Layer Gateways	
Avaya H.323	Not supported
Authentication with IC Series devices	
Layer 2 enforcement in UAC deployments	Not supported **NOTE**: UAC-IDP and UAC-UTM also are not supported.
Chassis cluster support **NOTE**: Support for chassis clustering to provide network node redundancy is only available on a vSRX deployment in Contrail, VMware, KVM, and Windows Hyper-V Server 2016.	
Chassis cluster for VirtIO driver	Only supported with KVM **NOTE**: The link status of VirtIO interfaces is always reported as UP, so a vSRX chassis cluster cannot receive link up and link down messages from VirtIO interfaces.
Dual control links	Not supported
In-band and low-impact cluster upgrades	Not supported
LAG and LACP (Layer 2 and Layer 3)	Not supported
Layer 2 Ethernet switching	Not supported
Low-latency firewall	Not supported
Class of service	

Table 6: SRX Series Features Not Supported on vSRX *(Continued)*

SRX Series Feature	vSRX Notes
High-priority queue on SPC	Not supported
Tunnels	Only GRE and IP-IP tunnels supported **NOTE**: A vSRX VM deployed on Microsoft Azure Cloud does not support GRE and multicast.
Data plane security log messages (stream mode)	
TLS protocol	Not supported
Diagnostic tools	
Flow monitoring cflowd version 9	Not supported
Ping Ethernet (CFM)	Not supported
Traceroute Ethernet (CFM)	Not supported
DNS proxy	
Dynamic DNS	Not supported
Ethernet link aggregation	
LACP in standalone or chassis cluster mode	Not supported
Layer 3 LAG on routed ports	Not supported
Static LAG in standalone or chassis cluster mode	Not supported

Table 6: SRX Series Features Not Supported on vSRX *(Continued)*

SRX Series Feature	vSRX Notes
Ethernet link fault management	
Physical interface (encapsulations) • **ethernet-ccc** • **ethernet-tcc** • **extended-vlan-ccc** • **extended-vlan-tcc**	Not supported
Interface family • **ccc, tcc** • **ethernet-switching**	Not supported
Flow-based and packet-based processing	
End-to-end packet debugging	Not supported
Network processor bundling	
Services offloading	
Interfaces	
Aggregated Ethernet interface	Not supported
IEEE 802.1X dynamic VLAN assignment	Not supported
IEEE 802.1X MAC bypass	Not supported

Table 6: SRX Series Features Not Supported on vSRX *(Continued)*

SRX Series Feature	vSRX Notes
IEEE 802.1X port-based authentication control with multisupplicant support	Not supported
Interleaving using MLFR	Not supported
PoE	Not supported
PPP interface	Not supported
PPPoE-based radio-to-router protocol	Not supported
PPPoE interface **NOTE**: Starting in Junos OS Release 15.1X49-D100 and Junos OS Release 17.4R1, the vSRX supports Point-to-Point Protocol over Ethernet (PPPoE) interface.	Not supported
Promiscuous mode on interfaces	Only supported if enabled on the hypervisor
IPSec and VPNs	
Acadia - Clientless VPN	Not supported
DVPN	Not supported
Hardware IPsec (bulk crypto) Cavium/RMI	Not supported
IPsec tunnel termination in routing instances	Supported on virtual router only
Multicast for AutoVPN	Not supported

Table 6: SRX Series Features Not Supported on vSRX *(Continued)*

SRX Series Feature	vSRX Notes
IPv6 support	
DS-Lite concentrator (also called Address Family Transition Router [AFTR])	Not supported
DS-Lite initiator (aka B4)	Not supported
J-Web	
Enhanced routing configuration	Not supported
New Setup wizard (for new configurations)	Not supported
PPPoE wizard	Not supported
Remote VPN wizard	Not supported
Rescue link on dashboard	Not supported
UTM configuration for Kaspersky antivirus and the default Web filtering profile	Not supported
Log file formats for system (control plane) logs	
Binary format (binary)	Not supported
WELF	Not supported
Miscellaneous	

Table 6: SRX Series Features Not Supported on vSRX *(Continued)*

SRX Series Feature	vSRX Notes
GPRS **NOTE**: Starting in Junos OS Release 15.1X49-D70 and Junos OS Release 17.3R1, vSRX supports GPRS.	Not supported
Hardware acceleration	Not supported
Logical systems	Not supported
Outbound SSH	Not supported
Remote instance access	Not supported
USB modem	Not supported
Wireless LAN	Not supported
MPLS	
Crcuit cross-connect (CCC) and translational cross-connect (TCC)	Not supported
Layer 2 VPNs for Ethernet connections	Only if promiscuous mode is enabled on the hypervisor
Network Address Translation	
Maximize persistent NAT bindings	Not supported
Packet capture	

Table 6: SRX Series Features Not Supported on vSRX *(Continued)*

SRX Series Feature	vSRX Notes
Packet capture	Only supported on physical interfaces and tunnel interfaces, such as *gr*, *ip*, and *st0*. Packet capture is not supported on redundant Ethernet interfaces (*reth*).
Routing	
BGP extensions for IPv6	Not supported
BGP Flowspec	Not supported
BGP route reflector	Not supported
CRTP	Not supported
Switching	
Layer 3 Q-in-Q VLAN tagging	Not supported
Transparent mode	
UTM	Not supported
Unified threat management	
Express AV	Not supported
Kaspersky AV	Not supported
Upgrading and rebooting	

Table 6: SRX Series Features Not Supported on vSRX *(Continued)*

SRX Series Feature	vSRX Notes
Autorecovery	Not supported
Boot instance configuration	Not supported
Boot instance recovery	Not supported
Dual-root partitioning	Not supported
OS rollback	Not supported
User interfaces	
NSM	Not supported
SRC application	Not supported
Junos Space Virtual Director	Only supported with VMware

2

CHAPTER

Installing vSRX in Google Cloud

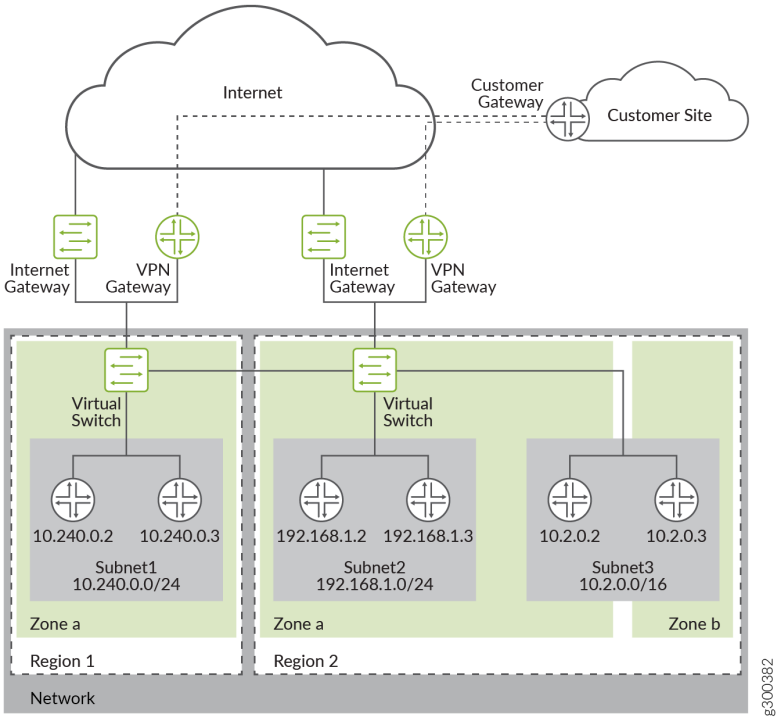
Prepare to setup vSRX Deployment on GCP

IN THIS SECTION

Before you begin, you need a Google account and an identity and access management (IAM) role, with all required permissions to access, create, modify, and delete Compute Engine Instances and Storage Service, and Google's VPC objects. You should also create access keys and corresponding secret access keys, certificates, and account identifiers.

Figure 4 on page 30 shows an example of how you can deploy vSRX to provide security for applications running in a private subnet of Google VPC.

Figure 4: Example of a Google VPC



You need to set up the vSRX 3.0 Firewall on Google Cloud Platform to deploy a vSRX 3.0 firewall on a Google Cloud Computer Engine instance on the Google Cloud Platform (GCP).

Before you deploy vSRX 3.0, you must create your project networks and subnetworks, and plan networks and IP address assignments for the vSRX interfaces. During the deployment, you must choose from the existing networks and subnetworks.

Subnetworks—You must create subnetworks in each VPC networks in specific region in which you plan to deploy the vSRX. A VPC Networks can add subnetworks in different region. These subnetworks are all internal network in GCP.

- **IP Address**—You need to assign IP address ranges when you create interface subnetworks.
- **Range**—The range for a network subnet cannot overlap with others.
- **External IP Address**—During vSRX deployment you can choose to enable or disable an external IP address when you create a network interface for the vSRX, by default, an ephemeral IP address is given, static IP address is not allowed, but after the deployment, you can change the external IP address from ephemeral address to a static IP address.

- **Management Interface**—The first network interface added to a vSRX is mapped to fxp0 on the vSRX.
  - Enable IP forwarding
  - This interface has an external IP address.
  - On vSRX, DHCP is enabled to fxp0 by default.
  - You can change the ephemeral IP address given during deployment to a static IP address, after you complete the deployment.
- **Interface Order**—First network interface is mapped to fxp0, second network interface is mapped to ge-0/0/0, 3rd network interface is mapped to ge-0/0/1.
- **Number of vSRX Interfaces**
  - The maximum number of virtual interfaces allowed per vSRX instance is 8.
  - To create a vSRX instance, you have to specify the machine type. The machine type specifies a particular collection of virtualized hardware resources available to a VM instance, including the memory size, virtual CPU count, and maximum disk capacity.
  - **Default VPC Network**—There is default network in a GCP project, you can delete the default network if unused. By default, 5 networks in a project. You can request additional networks for your project.
  - **Firewall Rules**—You must create a GCP firewall rules to allows access for management connection.

Before you begin, ensure to have the following ready:

- Google Cloud Platform Account Planning
- SSH Key Pair
- Virtual Private Cloud (VPC) Network Planning

Step 1: Google Cloud Platform Account Planning

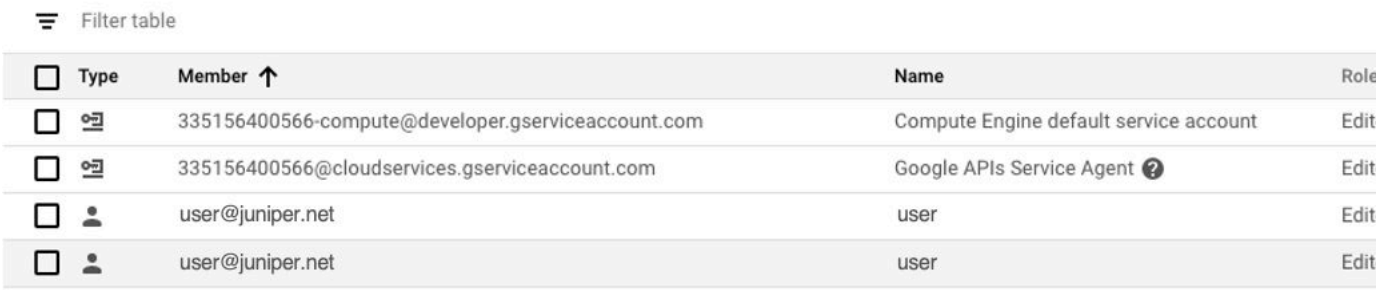
Before you begin deploying vSRX VM, review the licensing information and collect the information you'll need for the configuration process.

1. Understand your vSRX license requirements.
2. Determine private IP address for your management and other interfaces.
3. Get required permissions for the GCP account.

- GCP user account with a linked e-mail address
- Identity and access management (IAM) roles as Compute Viewer, Storage Object Viewer,and Monitoring Metric Writer.

Accounts and Permissions—Ensure you have proper accounts and permissions before your deploy vSRX 3.0 on a Google Computer Engine instance. Sample account roles and IAM permissions are shown in Figure 5 on page 32

Figure 5: Sample Account Roles and IAM Permissions



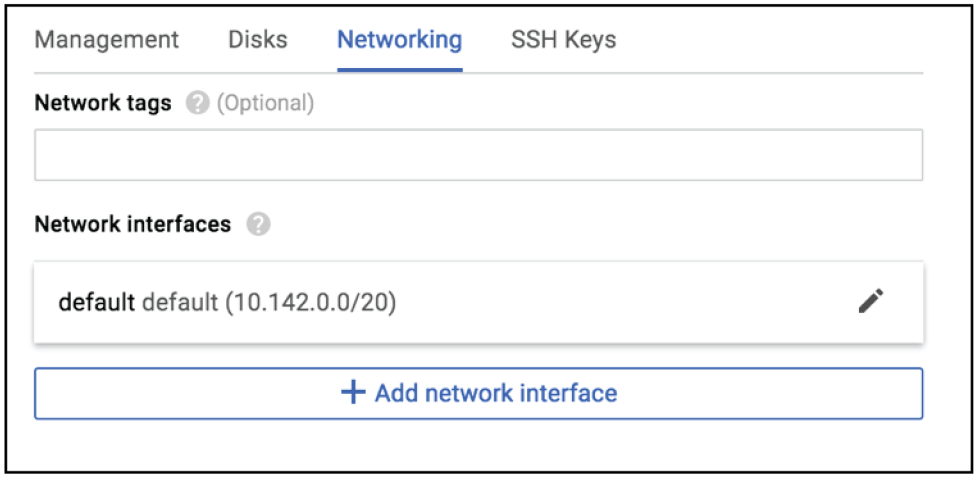
Step 2: Define Network Attributes and Generate SSH Key Pair for Authentication

The procedure below provides you steps to define network attributes and generate your own SSH Key pairs to allow your first time login:

1. After choosing the machine type, you must define networking attributes in the advanced options for the VM.

Click the **VM instances** tab on the home page and then click the **Networking** tab as shown in Figure 6 on page 33. Update the networking attributes and add the required interfaces.

Figure 6: Define Network Attributes



You can add up to 8 interfaces for each vSRX instance.

> **NOTE**: You cannot choose virtual interface type. GCP supports only the VirtIO interface type. SR-IOV is not supported in GCP.

2. vSRX manages authentication for first login only through RSA SSH key authentication. Password is not allowed, so you cannot log into vSRX through console on GCP web. Root login without password is not allowed. So you must generate your own SSH Key before your deploy a vSRX instance in Google Compute Engine.

   Generate the public key and the private key. Create an SSH key pair and store the SSH Key in the default location for your operation system.

   - If you are using Linux or MacOS: Use ssh-keygen to create the key pair in your .ssh directory. Run the **ssh-keygen -t rsa -f ~/.ssh/gcp-user-1 -C gcp-user** command. Here **gcp-user-1** is name of key file and **gcp-user** is username.

     > **NOTE**: It is mandatory to use “gcp-user” as username when you login to the vSRX for the first time vSRX.

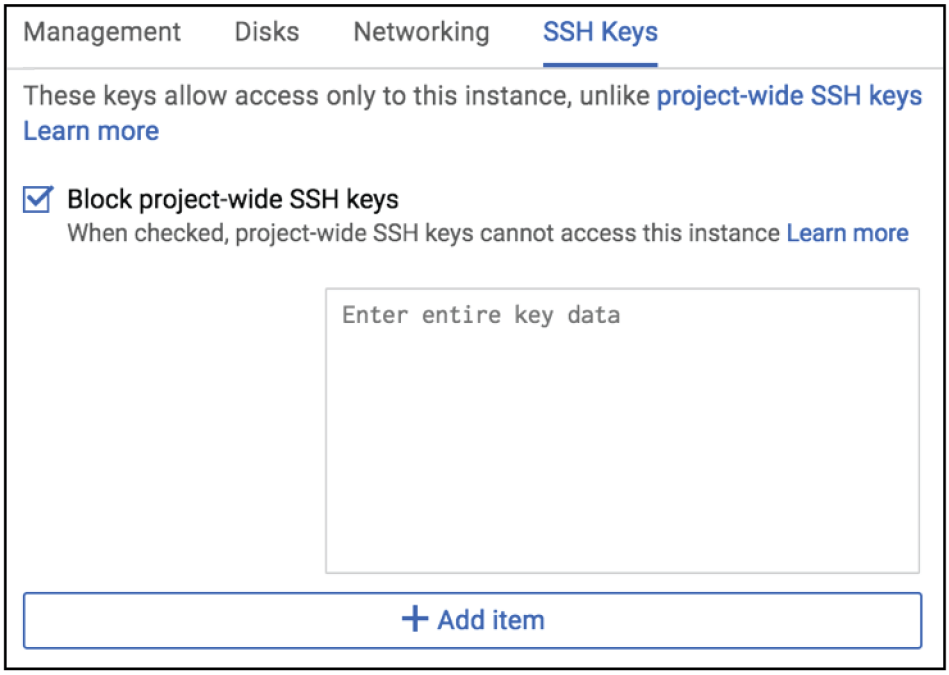
   - If you are using Windows: Use PuTTYgen to create the key pair.

3. Copy your public key in a text editor. You need to paste it later while deploying vSRX in the GCP Marketplace.
4. Block project-wide SSH keys and specify an SSH key for each vSRX instance.

   Click the **SSH Keys** tab on the **VM instances** page as shown in Figure 7 on page 34.

> **NOTE**: The SSH key is used by the public key authentication for the first login. As a security measurement, you must block project-wide SSH keys and specify an SSH key for each vSRX instance.

Figure 7: Block Project-Wide SSH Keys



5. Save your private key in .ppk format. You need this key later to authenticate the vSRX instance.

Step 3: Plan Google Virtual Private Cloud (VPC) Network

Prepare the virtual private cloud (VPC) networks in Google Cloud Platform. You must create virtual private networks, rules, and subnetworks and configure interfaces before you start deploying the vSRX on GCP which involves:

1. Log in to the Google Cloud console.
2. **VPC Networks**—You must create a custom network specifically for each vSRX network interface.
   In the left navigation area, click **VPC network** under **NETWORKING**.
3. On the top pane, click **CREATE VPC NETWORK**.
4. Enter a name for the network.
5. Create a subnetwork with the following details and click **Create**.
   - **Name**—Name of the subnetwork.
   - **IP Address**—Assign an IP address range for creating interface subnetworks. This range is used for your internal network, so ensure that the address range does not overlap with other subnets.
   - **Region**—Select the region where you want to launch your vSRX VM.
   - **Private Google Access**—Retain the default value **Off**.
   - **Flow logs**—Retain the default value **Off**.

Deploy vSRX in Google Cloud Platform

IN THIS SECTION

The following procedures describe how to deploy vSRX in the Google Virtual Private Cloud (VPC):

- Deploy the vSRX Firewall from Google Cloud Platform Marketplace.
- Use custom private image to deploy the vSRX Firewall from the GCP portal.
- Use cloud-init to deploy the vSRX Firewall through gcloud using CLI.

Deploy the vSRX Firewall from Marketplace Launcher

You can use the Google Cloud Platform Marketplace to deploy your vSRX3.0 with licenses as avirtual machine(VM) running on a Google Compute Engine instance.

Before you deploy the vSRX, you must create or choose a project in your organization and create any networks and subnets that will connect to the firewall. You cannot attach multiple network interfaces to the same VPC network. Every interface you create must have a dedicated network with at least one subnet.

This topic provide your step to deploy a vSRX Firewall from the Google Cloud Platform Marketplace Launcher.

1. Log in to the Google Cloud Platform console.
2. In the left navigation area, select **Marketplace**.
3. Locate the vSRX listing in the Marketplace.

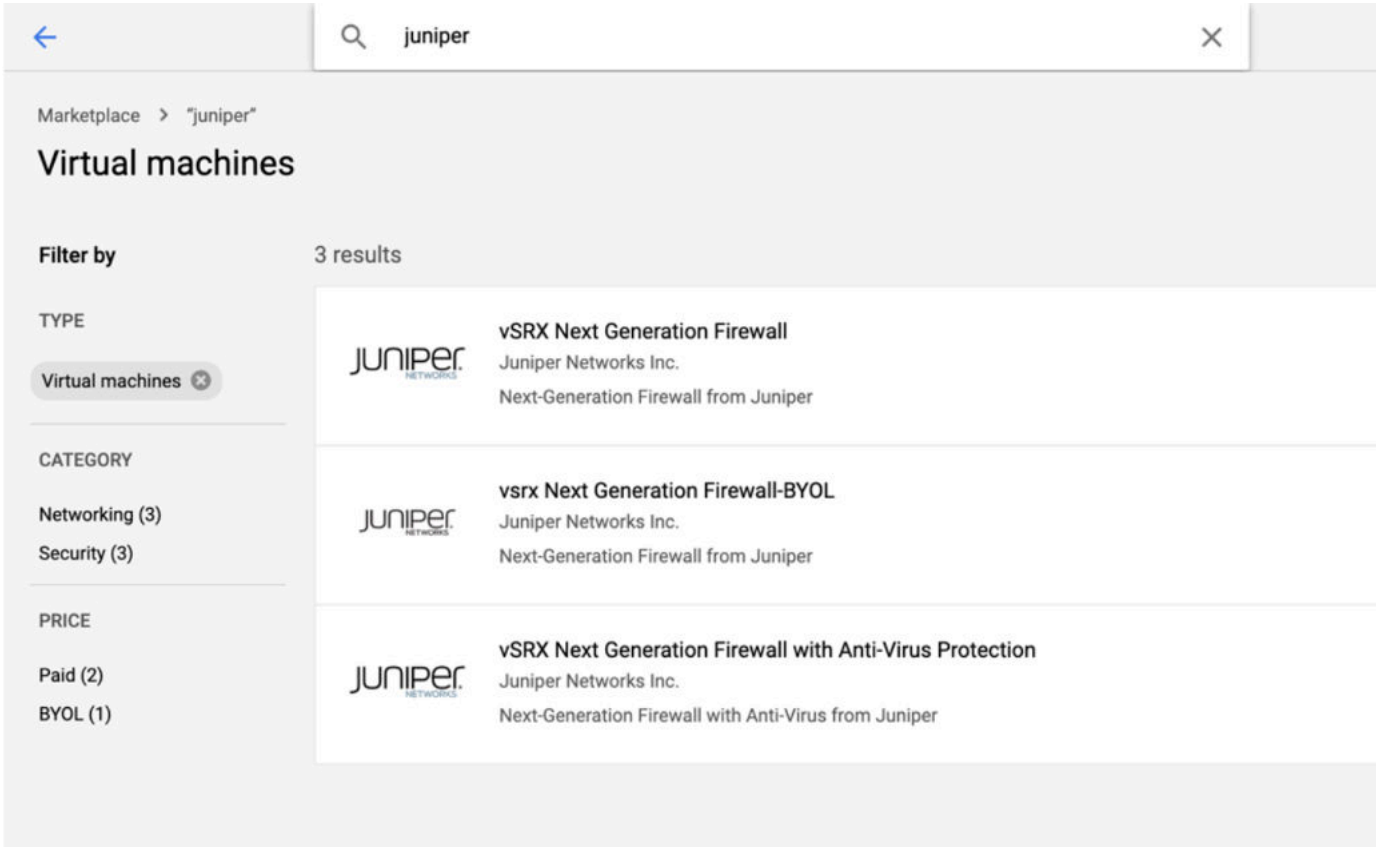
   In the Search box, type 'Juniper' or 'vSRX' and click one of the following options based on your licensing requirements as shown in Figure 8 on page 37.

   The images are available from cloud:

   - vSRX Next Generation Firewall
   - vsrx Next Generation Firewall-BYOL

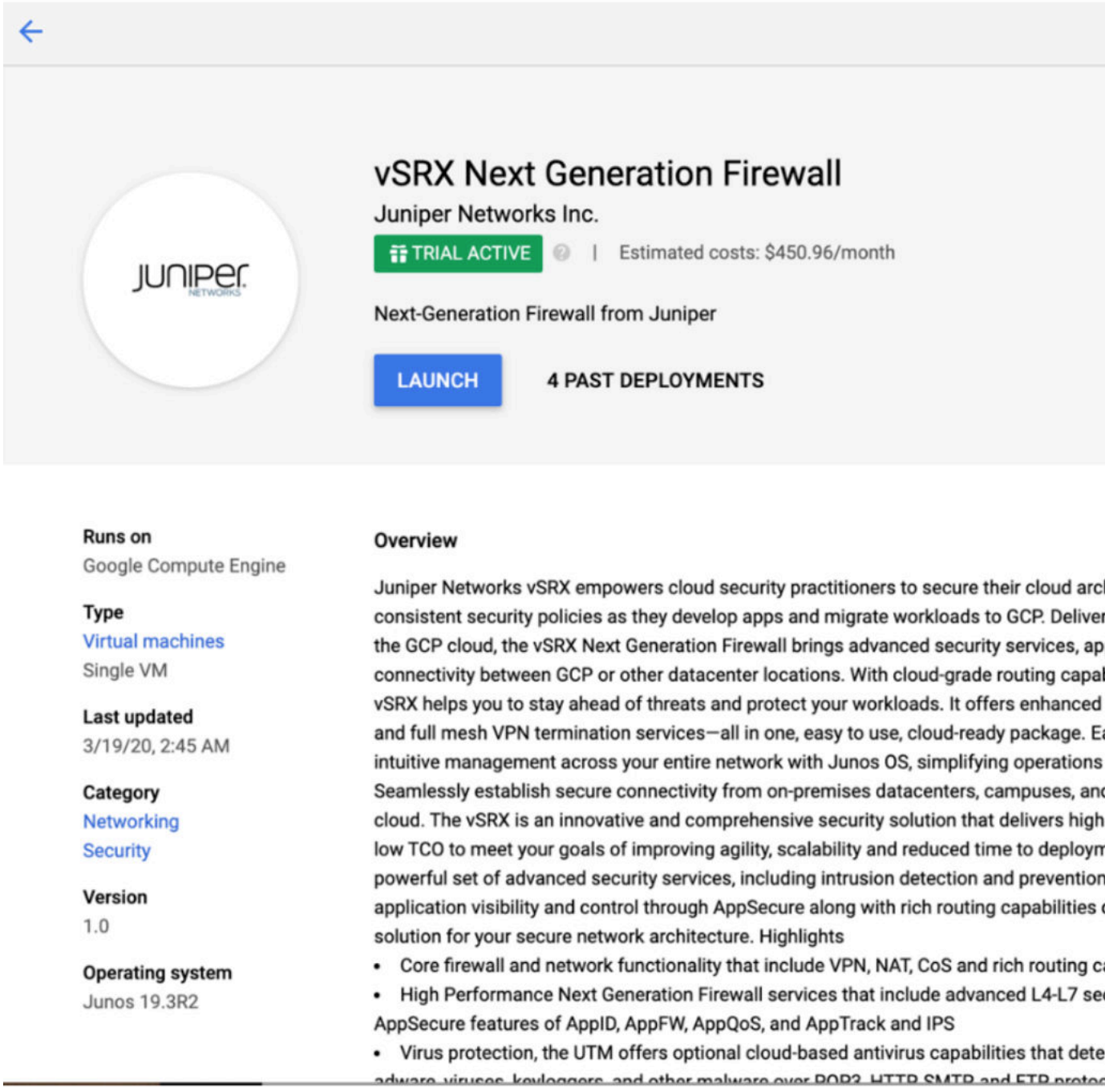
- vSRX Next Generation Firewall with Anti-Virus Protection

Figure 8: Locate vSRX Listing in the GCP Marketplace



4. Click **Launch** on Compute Engine. The deployment page appears as shown in Figure 9 on page 38.

Figure 9: Launch vSRX Instance in GCP from Marketplace



5. Name the instance and choose resources.

   Provide the details for the vSRX VM:

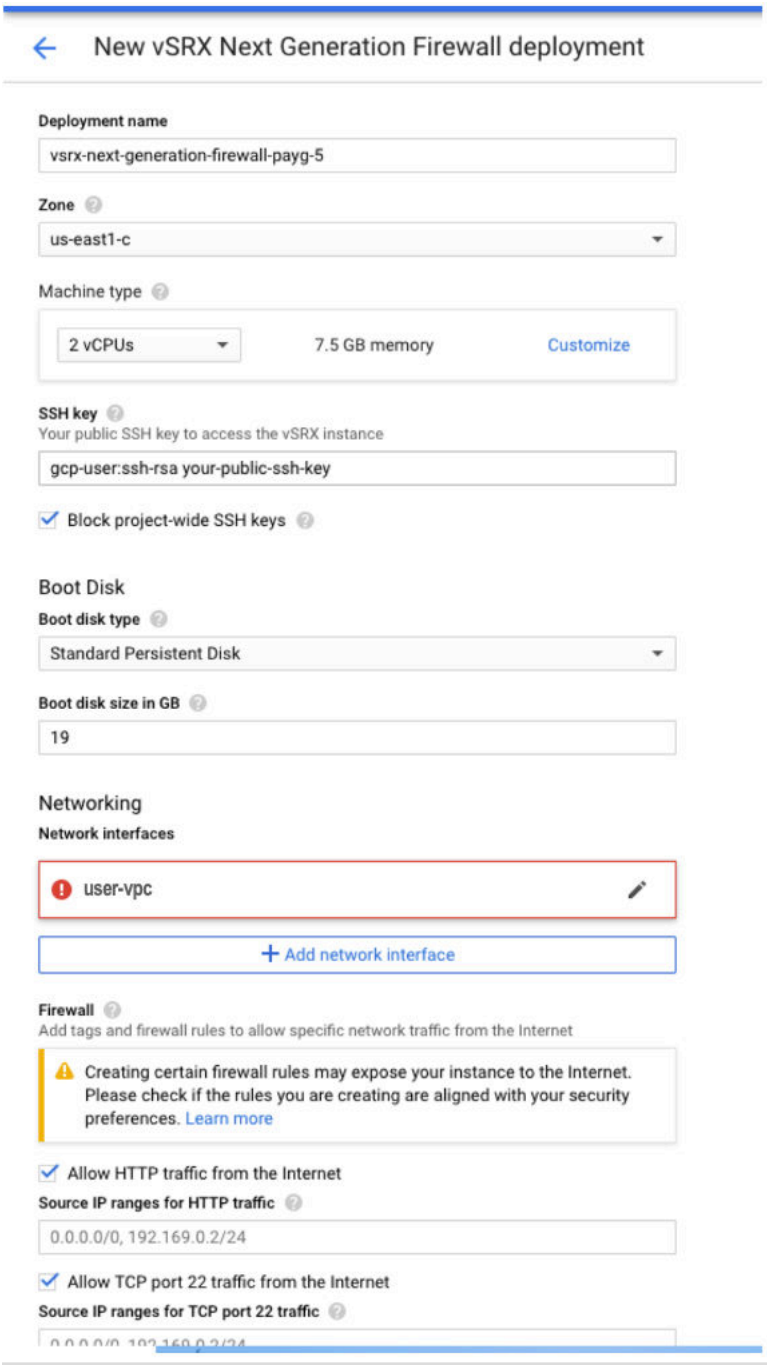
- **Deployment Name**—Enter a unique name for your vSRX VM.
- **Machine type**—Select a machine type based on the system requirements for your license.
- **SSH key**—Paste your public SSH key that you created earlier.
  - Paste the key after the text gcp-user:

    NOTE: It is mandatory to use “gcp-user” as username when you login to the vSRX for the first time vSRX.

  - Select the Block project-wide SSH keys option.
- **Network interfaces**—Select the VPC network and the subnets. Note that you can add only those subnets that you’ve created for the selected zone for this vSRX VM.
- **IP Forwarding**—Retain the default value On. This is a mandatory requirement for the vSRX VM.
- **Enable External IP**—Select the ephemeral option. This setting allows the GCP to provide an ephemeral IP address to act as the external IP address.
- **Allow HTTP traffic from the Internet**—Retain the default value as selected. We recommend not providing HTTP access unless absolutely necessary.
- **Allow TCP port 22 traffic from the Internet**—Retain the default value as selected. F or security reasons, we recommend that you limit the SSH access only to the specific IP address to access the vSRX

Name the instance and choose resources as shown in Figure 10 on page 40.

Figure 10: Name vSRX Instance and Choose Resources in GCP Marketplace



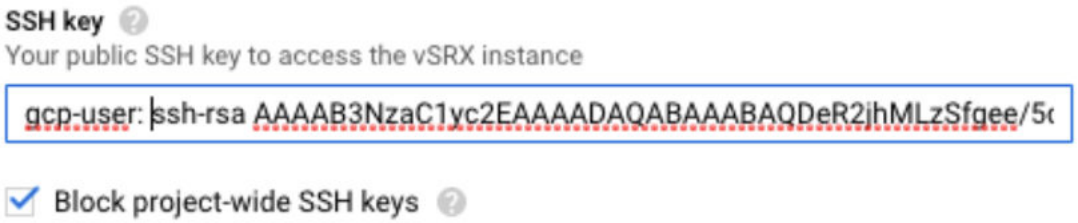
a. Choose a **Deployment Name**. The name must be unique and cannot conflict with any other deployment in the project.

b. Select a zone.

c. Select a machine type.

d. Set the SSH Key as shown in Figure 11 on page 41.

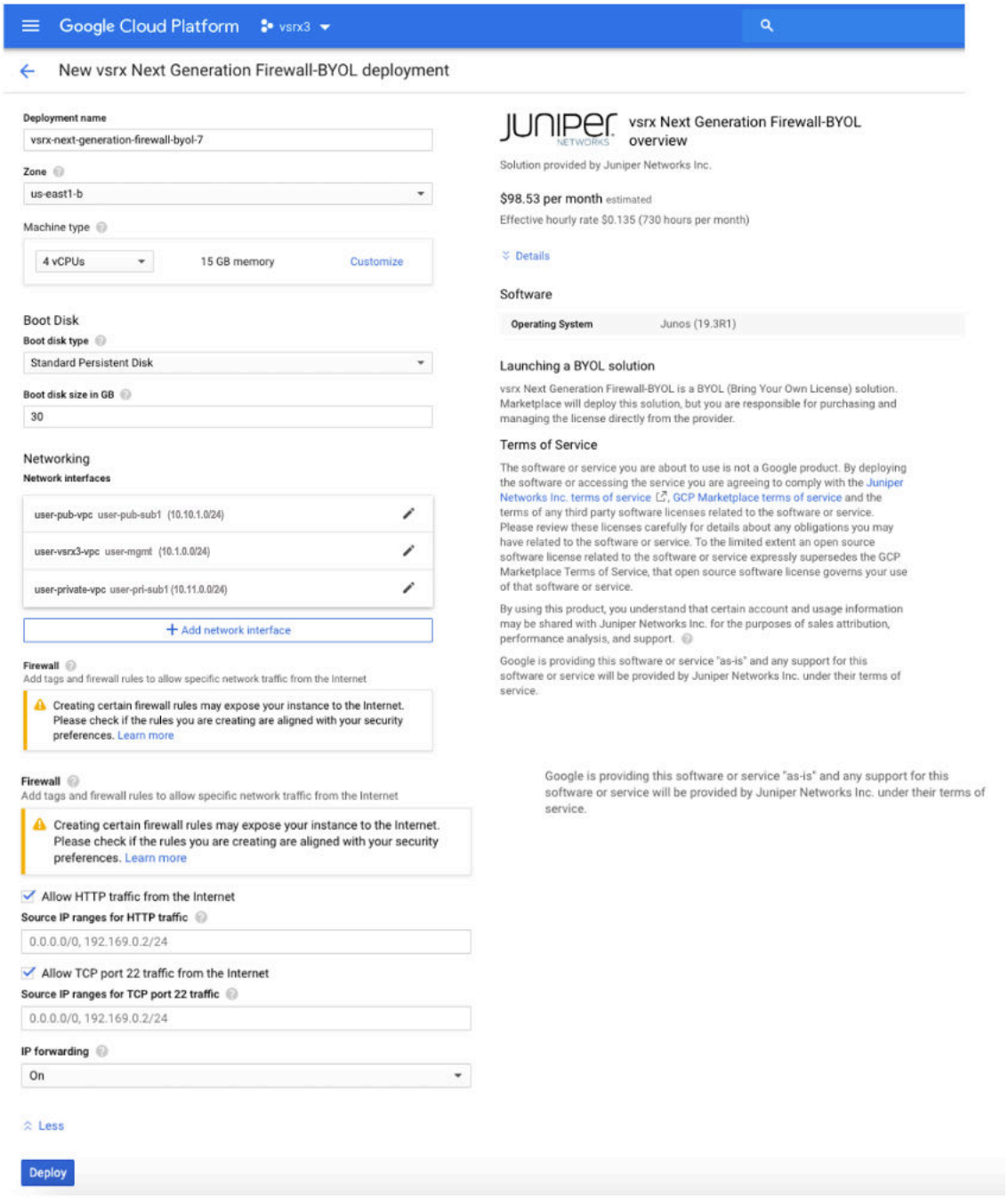
Figure 11: SSH Key



e. Configure the network and subnet.

f. Leave **IP forwarding** ‘on’ (mandatory for vSRX deployments) as shown in Figure 12 on page 42.

Figure 12: IP Forwarding Configuration



6. Accept GCP Marketplace **Terms of Service**.
7. Click **Deploy**.

The system shows the progress of your vSRX deployment. It displays a message indicating the successful completion of the deployment and sends you an e-mail notification for the same.

8. Click your VM to view the details. You can view your VM details by navigating to the Compute Engine under **COMPUTE** in the left navigation area.

   Make note of the external IP address, shown under Network interfaces. You'll need this address later to log on to your vSRX instance using the CLI.

9. Logging in to a vSRX Instance.

   In GCP deployments, vSRX instances provide the following capabilities by default to enhance security:

   - Allows you to login only through SSH.
   - cloud-init is used to setup SSH key login.
   - SSH password login is disabled for root account.

   > **NOTE**: Root login using SSH password is be disabled by default.

   Use an SSH client to log in to a vSRX instance for the first time. To log in, specify the location where you saved the SSH key pair file for the user account, and the IP address assigned to the vSRX management interface (fxp0).

   > **NOTE**: Root login using a Junos OS password is disabled by default. You can configure other users after the initial Junos OS setup phase.

   If you do not have the key pair filename and the IP address, use these steps to view the key pair name and IP for a vSRX instance:

   a. In the GCP portal, select **Instances**.

   b. Select the vSRX instance, and select **eth0** in the Description tab to view the IP address for the fxp0 management interface.

   c. Click **Connect** above the list of instances to view the SSH key pair filename.

   To configure the basic settings for the vSRX instance, see *Configure vSRX Using the CLI*.

   > **NOTE**: gcloud connect to vSRX is not supported. Always use ssh with user provided key to connect to vSRX after instance is up.

Deploy the vSRX Instance from GCP Portal Using Custom Private Image

IN THIS SECTION

You can also use your custom private image to deploy the vSRX instead of deploying an image from GCP marketplace. Firstly you need upload the private image to Google Cloud storage, then create compute image in GCP, and then deploy vSRX on Google Compute Engine.

Watch the video Deploying vSRX Virtual Firewalls on Google Cloud Platform to understand how you can deploy vSRX instances from GCP.

Upload vSRX Image to Google Cloud Storage

To upload vSRX image to Google Cloud Storage:

1. Prepare the private vSRX image file.

   A custom image is a boot disk image that is private to you. To import a disk image to Google Compute Engine, the image file must meet the following requirements.

   - Disk image filename must be **disk.raw**.
   - RAW image file must have a size in an increment of 1 GB. For example, the file must be either 10 GB or 11 GB but not 10.5 GB.
   - Compressed file must be a .tar.gz file that uses gzip compression and the GNU tar format.

   To use .qcow2 vSRX image to generate .tar.gz file follow below steps to process the upload.

   a. Convert .qcow2 to "disk.raw" (disk.raw is the dedicate name for google cloud deployment).

      qemu-img convert -f qcow2 -O raw junos-vsrx3-x86-64-19.2I-20190115_dev_common.0.1057.qcow2 disk.raw

   b. Compress to .tgz file.

      tar -czf vsrx-0115.tar.gz disk.raw

2. Upload image to Google Cloud Storage. You can upload your custom private image in two ways:

   - Upload image through SDK shell

- Upload image from Google Cloud Platform portal

Upload image through SDK shell:

Install Google Cloud SDK on Ubuntu.

You must install Google Cloud SDK on your operation system. below is the sample to install it on Ubuntu.

For more information on Google Cloud SDK installation on Ubuntu, see https://cloud.google.com/sdk/docs/quickstart-debian-ubuntu and for Gcloud command-line tool overview, see https://cloud.google.com/sdk/gcloud/.

To upload image through SDK shell:

1. Create google cloud storage.

   gs://vsrx-image

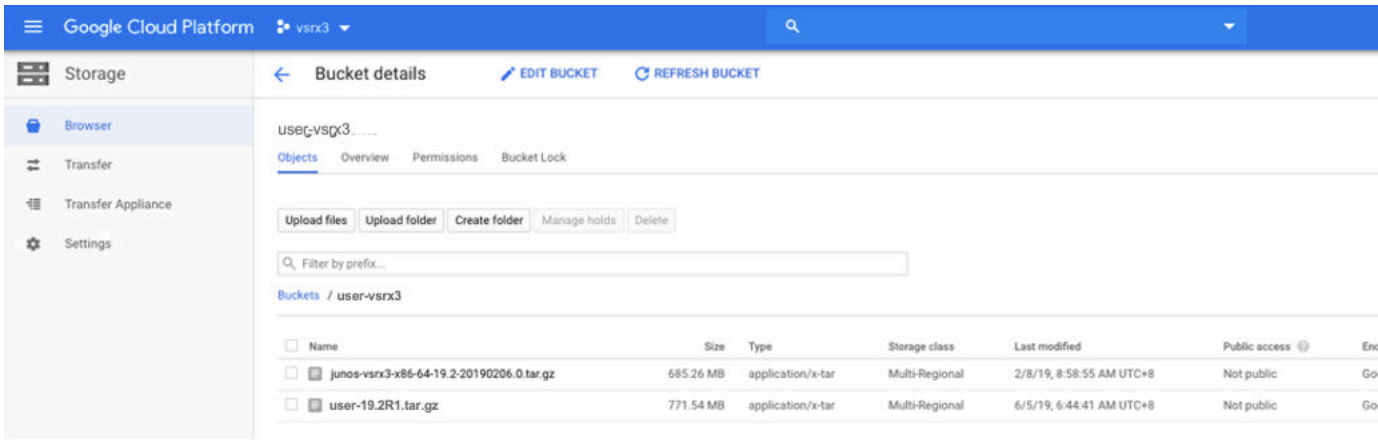
2. Copy disk.raw to cloud storage.

   gsutil cp vsrx-0115.tar.gz gs://vsrx-image

To upload image from Google Cloud Platform portal.

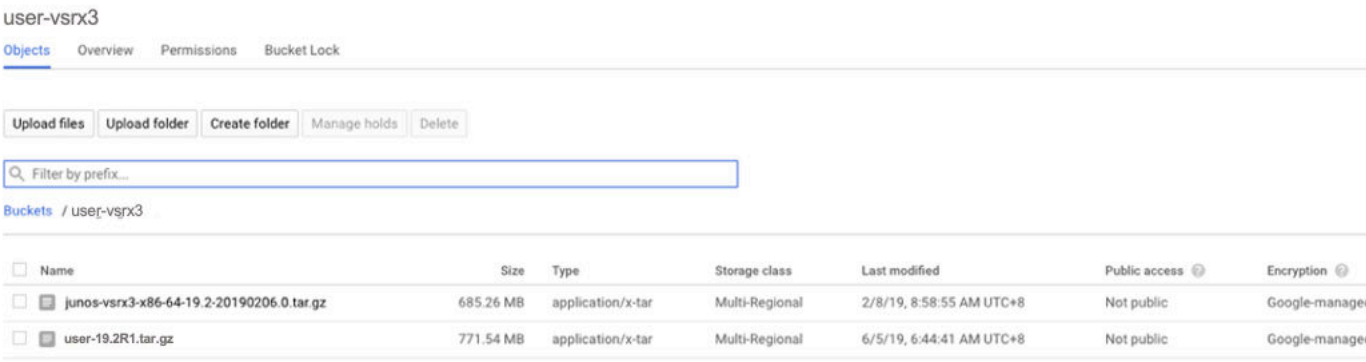
1. Click **Storage->Create Bucket->Upload files** as shown in Figure 13 on page 45.

Figure 13: vSRX Image Upload from GCP Portal



2. Check the private image is available in Google Cloud Storage by selecting **Storage -> Bucket detail** in Google Cloud Platform web as shown in Figure 14 on page 46.

Figure 14: View Private Images in GCP Portal



Create vSRX Image

After you upload the vSRX image file to GCP storage you need to create GCP compute image for vSRX deployment.

1. Create image in cloud.

   A sample to create vSRX image using the package ready in GCP project storage is shown below. The option of 'multi_ip_subnet' is mandatory.

   gcloud compute images create vsrx-0115 '--guest-os-features=multi_ip_subnet' --source-uri=gs://vsrx-image/vsrx-0115.tar.gz

2. Check the private image is available in Google Cloud Compute Engine.

   root@cnrd-ubuntu173:~# gcloud compute images list | grep vsrx3-194* vsrx-0115. vsrx3-218606 READY

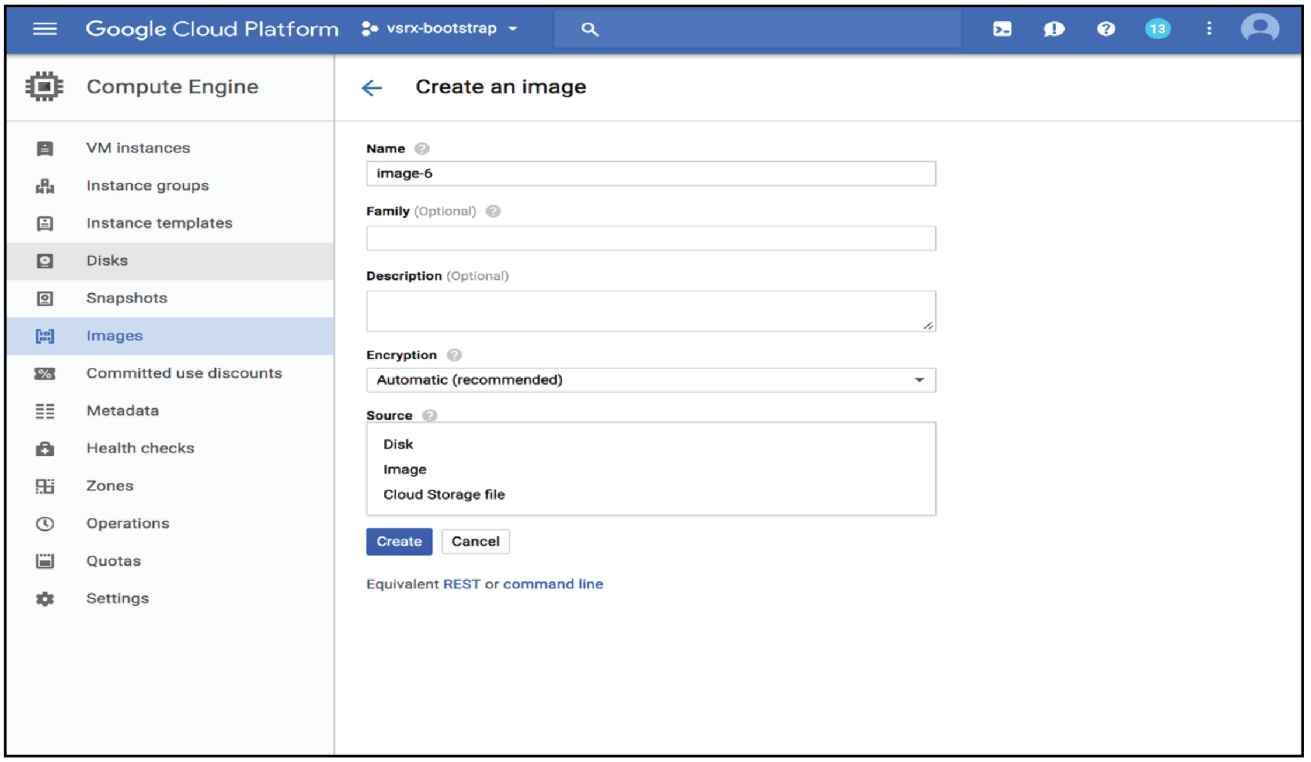
Using Google Console

You can rename the image file using the Google console as well.

1. Log in to your Google account and open the **Google Cloud Platform** home page.

2. Click the**images** option on the **Google Cloud Platform** page. The **Create an image** page opens as shown in Figure 15 on page 47

Figure 15: Google Cloud Platform Image Creation Page

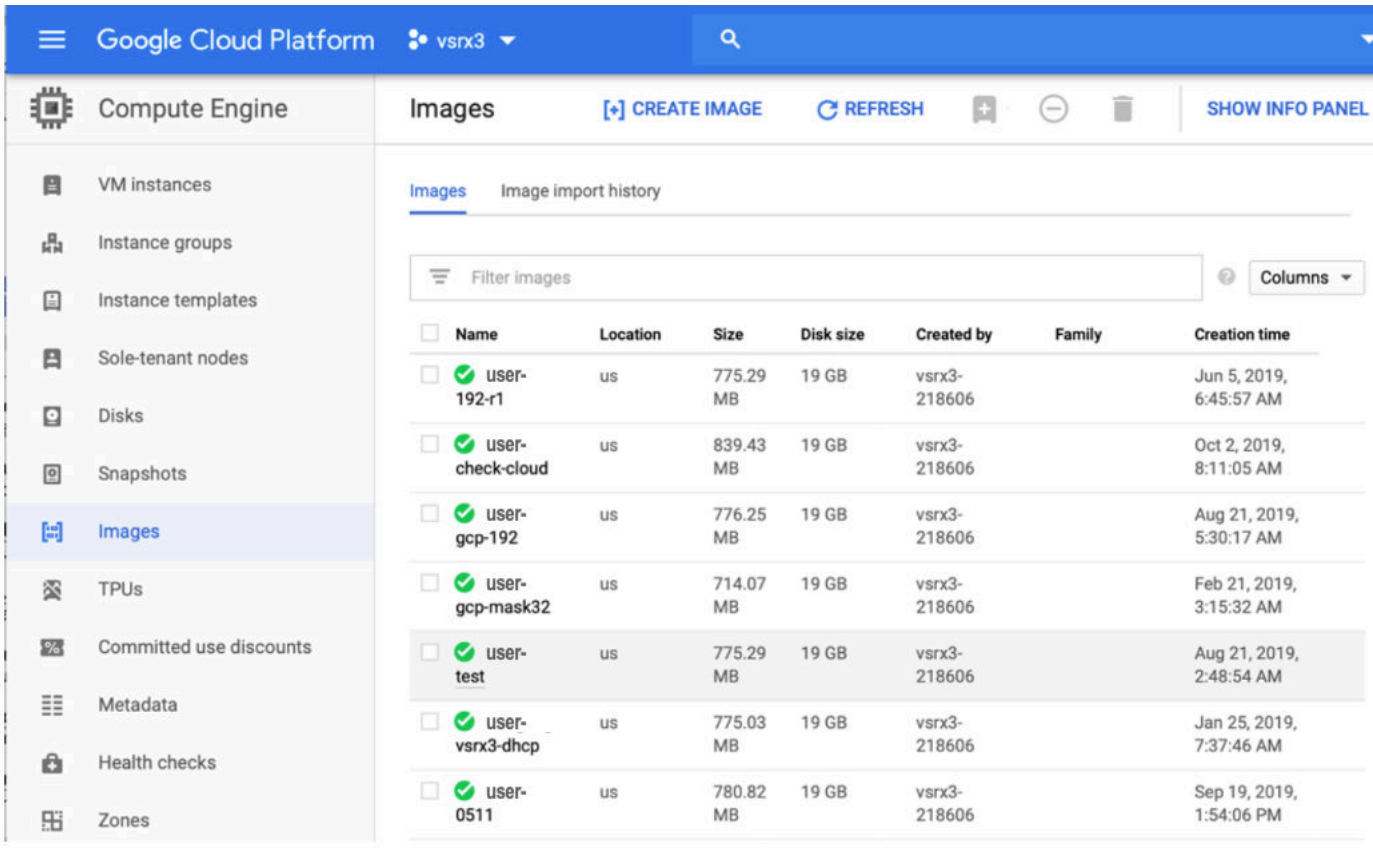


3. Fill in the required details in the **Create an image** page and click **Create**.

> **NOTE**: It is mandatory to use “gcp-user” as username when you login to the vSRX for the first time vSRX.

4. Check the private image that available in Google Cloud Compute Engine. On Google Cloud Platform web, click **Compute Engine**->**Images** as shown in Figure 16 on page 48.

Figure 16: Check Private Image in Google Cloud Compute Engine



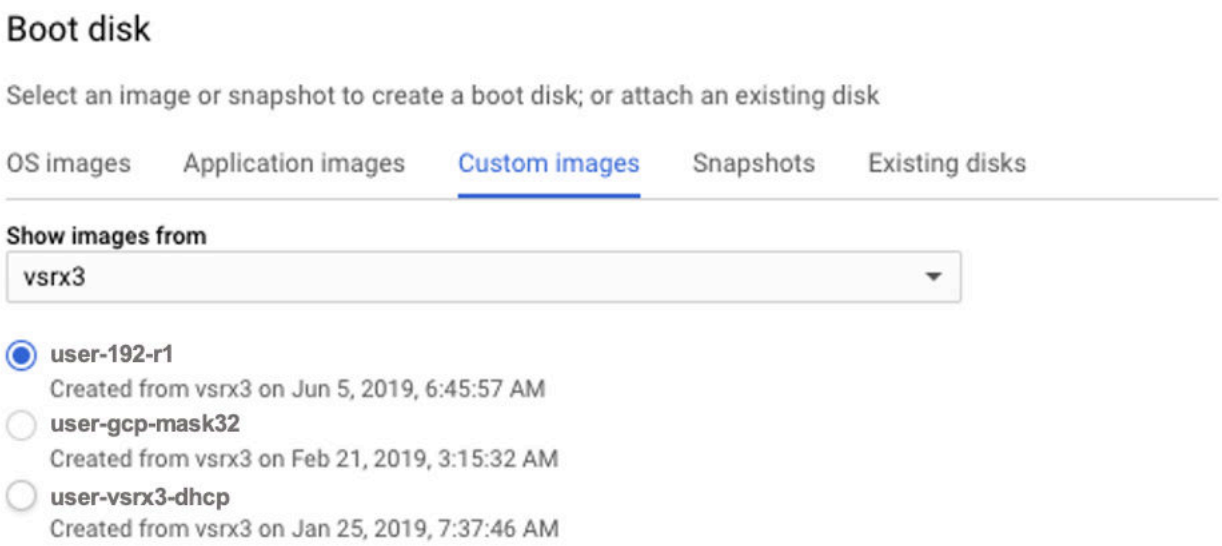
Deploy the vSRX Firewall from GCP Portal

You can follow below steps to deploy a vSRX instance:

1. Login Google Cloud Platform portal, go to **Compute Engine -> VM instances** and click **CREATE INSTANCE**.
2. Configure a vSRX instance.
   - **Name**—Specify a unique name to the instance.
   - **Region**—Select proper region you want to deploy the vSRX on, you must already create subnet in same region in proper VPC networks.
   - **Machine configuration** —Choose correct machine type.

- **Container** —Uncheck
- **Boot Disk**—Choose the private image in **Custom Images** tab as shown in Figure 17 on page 49. You must already upload the private image to Google Cloud Storage.

Figure 17: Boot Disk from Custom Images



- **Identity and API access**—Set default
- **Firewall / Management** —Set default
- **Firewall / Security**—Paste your SSH Key pair here. Details please reference “Prepare to setup vSRX on GCP – SSH Key”.
- **Firewall / Disks**—Set default
- **Firewall / Networking**:

Table 7: Firewall Networking

Firewall / Networking	Details
Hostname	Optional, you can specify tags for the instance used for route configuration.

Network Interfaces	Default
	You can set interfaces to existing VPC networks and subnet in same region. Interface number, Interface order and manage interface setting.

3. Click **Create**
4. Logging in to a vSRX Instance.

   In GCP deployments, vSRX instances provide the following capabilities by default to enhance security:

   - Allows you to login only through SSH.
   - SSH password login is disabled for root account.

   NOTE: Root login using a Junos OS password or SSH password is disabled by default. You can configure other users after the initial Junos OS setup phase.

   Use an SSH client to log in to a vSRX instance for the first time. To log in, specify the location where you saved the SSH key pair file for the user account, and the IP address assigned to the vSRX management interface (fxp0).

   NOTE: It is mandatory to use “gcp-user” as username when you login to the vSRX for the first time vSRX.

   If you do not have the key pair filename and the IP address, use these steps to view the key pair name and IP for a vSRX instance:

   a. In the GCP portal, select **Instances**.

   b. Select the vSRX instance, and select **eth0** in the Description tab to view the IP address for the fxp0 management interface.

   c. Click **Connect** above the list of instances to view the SSH key pair filename.

   To configure the basic settings for the vSRX instance, see *Configure vSRX Using the CLI*.

NOTE: gcloud connect to vSRX is not supported. Always use ssh with user provided key to connect to vSRX after instance is up.

Deploy the vSRX Firewall Using Cloud-init

vSRX supports cloud-init. Cloud-init is an open-source multi-distribution package that handles early initialization of a cloud instance. It allows user to customize VM instance with attributes like hostname and default IP on the first boot. Cloud-init is particularly useful when user wants to deploy large number of VM instances in the data center using automation tools.

Some of the initial provisioning parameters for first boot are:

- Hostname
- Root password
- SSH public key

NOTE: for the ssh key file, it needs to be in the format "<username>:<key value>" as required by google cloud. Something like this:

- Management interface (fxp0) IP
- Default gateway IP

You can deploy vSRX Firewall using cloud-init in two ways:

- From Google SDK
- To deploy vSRX with cloud-init from Google portal, see "Deploy the vSRX Firewall from GCP Portal" on page 48. To add user-data to have cloud init enabled specify the metadata.

GCE supports cloud-init type instance configuration. To launch instance with user data, use the command below as an example.

Figure 18: Sample Cloud-Init Configuration

```
gcloud compute instances create vsrx-cloudinit-001 --image vsrx-0115 \
--zone=us-west1-b \
--network-interface address=,network=vpc-1-mgt,subnet=subnet-1-uswest1-5  \
--network-interface address=,network=vpc-untrust-global,subnet=subnet-6-
uswest1-16,private-network-ip=10.16.16.113 \
--network-interface no-address,network=vpc-trust-regional,subnet=subnet-7-
uswest1-26,private-network-ip=10.26.26.113 \
--machine-type=n1-standard-4 --can-ip-forward \
--metadata-from-file user-data=junos.conf,ssh-keys=gcp-user.pub
```

Please note the following points:

- junos.conf is configuration file with '#junos-config' in content
- gcp-user.pub is ssh public key
- vSRX 3.0 supports RSA key pair only
- For the SSH key file, it needs to be in the format **<username>:<key value>** as required by Google cloud. Refer the sample SSH key file below.

```
root@cnrd-kvmsrv37:~# cat gcp-user.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDeR2jhMLzSfgee/5cnduTa+13yVLKbTa/
OFnZSHQsZoA5LKHIXs/
TbyooZTX5PnfNr6hx2Iyxjaodu01kT0UJ87wps8n9BH74DP6x0YK07OaZZl5T/
5Iso9fXRCzl9+go9vKzNKhqXmqKUc3Fl6hTX2QzQbtrwN2twLzCxz+OSliCoobJr+/
8wPcvI6fUbL6FRTgE1zC1HBlDKspK7x47YDYPJlUcyMhRtGvxd319jrx5i96mZq850+
dCfZkHSipT09hFRtk8C4MsOaKsw3RWUCY5LCPekrutrLLfhMKh88onv4ud7gXOklSwgVVod49aY2Ff
iaACMAVoaomfYXweP
gcp-user



ssh -i <private-key> gcp-user@<vSRX management public ip>
```

- In junos.conf, please remove the “gcp-default” block in your user data. They will shadow the one created by vSRX init script. Refer the sample junos config

```
    #junos-config
security {
    policies {
        default-policy {
            permit-all;
        }
    }
    zones {
        security-zone trust {
            interfaces {
                ge-0/0/0.0;
            }
        }
        security-zone untrust {
            interfaces {
                ge-0/0/1.0;
            }
        }
    }
}
interfaces {
    ge-0/0/0 {
        unit 0 {
            family inet {
                10.0.0.10/24;
            }
        }
    }
    ge-0/0/1 {
        unit 0 {
            family inet {
                10.0.1.10/24;
            }
        }
    }
}
```

NOTE: gcloud connect to vSRX is not supported. Always use ssh with user provided key to connect to vSRX after instance is up.

RELATED DOCUMENTATION

Deploying vSRX Virtual Firewalls on Google Cloud Platform

Upgrade the Junos OS for vSRX Software Release

You can upgrade the Junos OS for vSRX software using the CLI. Upgrading or downgrading Junos OS can take several hours, depending on the size and configuration of the network. Download the desired Junos OS Release for the **vSRX.tgz** file from the Juniper Networks website.

You also can upgrade using J-Web (see J-Web) or the Junos Space Network Management Platform (see Junos Space).

For the procedure on upgrading a specific Junos OS for vSRX software release, see the *Migration, Upgrade, and Downgrade Instructions* topic in the release-specific *vSRX Release Notes* available on the vSRX TechLibrary webpage.

CHAPTER 3

Configuring and Managing vSRX

vSRX Configuration and Management Tools

SUMMARY

This topic provides an overview of the various tools available to configure and manage a vSRX VM once it has been successfully deployed.

IN THIS SECTION

Understanding the Junos OS CLI and Junos Scripts

Junos OS CLI is a Juniper Networks specific command shell that runs on top of a UNIX-based operating system kernel.

Built into Junos OS, Junos script automation is an onboard toolset available on all Junos OS platforms, including routers, switches, and security devices running Junos OS (such as a vSRX instance).

You can use the Junos OS CLI and the Junos OS scripts to configure, manage, administer, and troubleshoot vSRX.

Understanding the J-Web Interface

The *J-Web* interface allows you to monitor, configure, troubleshoot, and manage vSRX instances by means of a Web browser. J-Web provides access to all the configuration statements supported by the vSRX instance.

Understanding Junos Space Security Director

As one of the Junos Space Network Management Platform applications, Junos Space Security Director helps organizations improve the reach, ease, and accuracy of security policy administration with a scalable, GUI-based management tool. Security Director automates security provisioning of a vSRX

instance through one centralized Web-based interface to help administrators manage all phases of the security policy life cycle more quickly and intuitively, from policy creation to remediation.

RELATED DOCUMENTATION

- CLI User Interface Overview
- J-Web Overview
- Security Director
- Mastering Junos Automation Programming
- Spotlight Secure Threat Intelligence

Configure vSRX Using the CLI

To configure the vSRX instance using the CLI:

1. Verify that the instance is powered on.
2. Log in using the username and password credentials for your vSRX VM deployment.
3. Start the CLI.

```
root#cli
root@>
```

4. Enter configuration mode.

```
configure
[edit]
root@#
```

5. Set the root authentication password by entering a *cleartext* password, an encrypted password, or an SSH public key string (*DSA* or *RSA*).

```
[edit]
root@# set system root-authentication plain-text-password
New password: password
Retype new password: password
```

6. Configure the traffic interfaces.

```
[edit]
root@# set interfaces ge-0/0/0 unit 0 family inet address assigned_ip/netmask
root@# set interfaces ge-0/0/1 unit 0 family inet address assigned_ip/netmask
```

> **NOTE**: Configuration of the management interface fxp0 for the vSRX is not necessary, because it is configured during vSRX VM deployment. Do not change the configuration for interface fxp0 and the default routing table or you will lose connectivity.

7. Configure routing interfaces to isolate management network and traffic network.

```
[edit]
root@# set routing-instances vsrx-vr1 instance-type virtual-router
root@# set routing-instances vsrx-vr1 interface ge-0/0/0.0
root@# set routing-instances vsrx-vr1 interface ge-0/0/1.0
```

8. Verify the configuration changes.

```
[edit]
root@# commit check
configuration check succeeds
```

9. Commit the current configuration to make it permanent and to avoid the possibility of losing connectivity to the vSRX instance.

```
[edit]
root@# commit confirmed
commit confirmed will be automatically rolled back in 10 minutes unless
confirmed
commit complete
# commit confirmed will be rolled back in 10 minutes
```

10. Commit the configuration to activate it on the instance.

```
[edit]
root@# commit
commit complete
```

11. Optionally, use the **show** command to display the configuration to verify that it is correct.

NOTE: Certain Junos OS software features require a license to activate the feature. To enable a licensed feature, you need to purchase, install, manage, and verify a license key that corresponds to each licensed feature. To conform to software feature licensing requirements, you must purchase one license per feature per instance. The presence of the appropriate software unlocking key on your virtual instance allows you to configure and use the licensed feature. See Managing Licenses for vSRX for details.

RELATED DOCUMENTATION

- Junos OS for SRX Series
- CLI User Guide

Configure vSRX Using the J-Web Interface

IN THIS SECTION

Access the J-Web Interface and Configuring vSRX

Use the Junos OS CLI to configure, at a minimum, the following parameters before you can access a vSRX VM using J-Web:

> ⚠ **CAUTION**: Do not change the configuration for interface fxp0 and default routing table or you will lose connectivity to the vSRX instance.

To configure vSRX using the *J-Web* Interface:

1. Launch a Web browser from the management instance.
2. Enter the vSRX fxp0 interface IP address in the Address box.
3. Specify the username and password.
4. Click **Log In**, and select the **Configuration Wizards** tab from the left navigation panel. The J-Web Setup wizard page opens.
5. Click **Setup**.

   You can use the Setup wizard to configure the vSRX VM or edit an existing configuration.

   - Select **Edit Existing Configuration** if you have already configured the wizard using the factory mode.
   - Select **Create New Configuration** to configure the vSRX VM using the wizard.

     The following configuration options are available in the guided setup:

     - Basic

       Select **basic** to configure the vSRX VM name and user account information as shown in Table 8 on page 60.

       - Instance name and user account options

         Table 8: Instance Name and User Account Information

Field	Description
Instance name	Type the name of the instance. For example: **vSRX**.

Table 8: Instance Name and User Account Information *(Continued)*

Field	Description
Root password	Create a default root user password.
Verify password	Verify the default root user password.
Operator	Add an optional administrative account in addition to the root account. User role options include: • **Super User**: This user has full system administration rights and can add, modify, and delete settings and users. • **Operator**: This user can perform system operations such as a system reset but cannot change the configuration or add or modify users. • **Read only**: This user can only access the system and view the configuration. • **Disabled**: This user cannot access the system.

- Select either **Time Server** or **Manual**. Table 9 on page 61 lists the system time options.

Table 9: System Time Options

Field	Description
Time Server	
Host Name	Type the hostname of the time server. For example: **ntp.example.com**.
IP	Type the IP address of the time server in the IP address entry field. For example: **192.0.2.254**.
NOTE: You can enter either the hostname or the IP address.	

Table 9: System Time Options *(Continued)*

Field	Description
Manual	
Date	Click the current date in the calendar.
Time	Set the hour, minute, and seconds. Choose **AM** or **PM**.
Time Zone (mandatory)	
Time Zone	Select the time zone from the list. For example: GMT Greenwich Mean Time GMT.

- Expert

  a. Select **Expert** to configure the basic options as well as the following advanced options:

  - Four or more internal zones
  - Internal zone services
  - Application of security policies between internal zones

  b. Click the **Need Help** icon for detailed configuration information.

  You see a success message after the basic configuration is complete.

Apply the Configuration

To apply the configuration settings for vSRX:

1. Review and ensure that the configuration settings are correct, and click **Next**. The Commit Configuration page appears.
2. Click **Apply Settings** to apply the configuration changes to vSRX.
3. Check the connectivity to the vSRX instance because you might lose connectivity if you have changed the management zone IP. Click the URL for reconnection instructions on how to reconnect to the instance.
4. Click **Done** to complete the setup.

After successful completion of the setup, you are redirected to the J-Web interface.

> **CAUTION**: After you complete the initial setup, you can relaunch the J-Web Setup wizard by clicking **Configuration>Setup**. You can either edit an existing configuration or create a new configuration. If you create a new configuration, the current configuration in vSRX will be deleted.

Add vSRX Feature Licenses

Certain Junos OS software features require a license to activate the feature. To enable a licensed feature, you need to purchase, install, manage, and verify a license key that corresponds to each licensed feature. To conform to software feature licensing requirements, you must purchase one license per feature per instance. The presence of the appropriate software unlocking key on your virtual instance allows you to configure and use the licensed feature.

To understand more about vSRX Licenses, see, Licenses for vSRX. Please refer to the Licensing Guide for general information about License Management. Please refer to the product Data Sheets for further details, or contact your Juniper Account Team or Juniper Partner.

Managing Security Policies for Virtual Machines Using Junos Space Security Director

SUMMARY

This topic provides you an overview of how you can manage security policies for VMs using security director.

Security Director is a Junos Space management application designed to enable quick, consistent, and accurate creation, maintenance, and application of network security policies for your security devices, including vSRX instances. With Security Director, you can configure security-related policy management including IPsec VPNs, firewall policies, NAT policies, IPS policies, and UTM policies. and push the configurations to your security devices. These configurations use objects such as addresses, services,

NAT pools, application signatures, policy profiles, VPN profiles, template definitions, and templates. These objects can be shared across multiple security configurations; shared objects can be created and used across many security policies and devices. You can create these objects prior to creating security configurations.

When you finish creating and verifying your security configurations from Security Director, you can publish these configurations and keep them ready to be pushed to all security devices, including vSRX instances, from a single interface.

The Configure tab is the workspace where all of the security configuration happens. You can configure firewall, IPS, NAT, and UTM policies; assign policies to devices; create and apply policy schedules; create and manage VPNs; and create and manage all the shared objects needed for managing your network security.

RELATED DOCUMENTATION

- Security Director

CHAPTER 4

vSRX in Google Cloud Use Cases

Example: Configuring NAT for vSRX

IN THIS SECTION

This example shows how to configure vSRX to NAT all hosts behind the vSRX instance in the Google Virtual Private Cloud (VPC) to the IP address of the vSRX egress interface on the untrust zone. This configuration allows hosts behind vSRX in a cloud network to access the Internet.

Before You Begin

Ensure that you have installed and launched a vSRX instance in a Google VPC.

Overview

A common cloud configuration includes hosts that you want to grant access to the Internet, but you do not want anyone from outside your cloud to get access to your hosts. You can use vSRX in a Google VPC to NAT traffic inside the Google VPC from the public Internet.

Configuring NAT

IN THIS SECTION

Procedure

Step-by-Step Procedure

To configure NAT on the vSRX instance:

1. Log in to the vSRX console in configuration edit mode (See *Configure vSRX Using the CLI*.
2. Set the IP addresses for vSRX revenue interfaces.

```
set interfaces ge-0/0/0 unit 0 family inet address 10.0.10.197/24
set interfaces ge-0/0/1 unit 0 family inet address 10.0.20.1/24
```

3. Set up the untrust security zone.

```
set security zones security-zone untrust host-inbound-traffic system-services https
set security zones security-zone untrust host-inbound-traffic system-services ssh
set security zones security-zone untrust interfaces ge-0/0/0.0
```

4. Set up the trust security zone.

```
set security zones security-zone trust host-inbound-traffic system-services https
set security zones security-zone trust host-inbound-traffic system-services ssh
set security zones security-zone trust host-inbound-traffic system-services ping
set security zones security-zone trust interfaces ge-0/0/1.0
```

5. Set up the security policies.

```
set security policies from-zone trust to-zone untrust policy test match source-address any
set security policies from-zone trust to-zone untrust policy test match destination-address any
set security policies from-zone trust to-zone untrust policy test match application any
set security policies from-zone trust to-zone untrust policy test then permit
```

6. Configure NAT.

```
set security nat source rule-set SNAT_RuleSet from zone trust
set security nat source rule-set SNAT_RuleSet to zone untrust
set security nat source rule-set SNAT_RuleSet rule SNAT_Rule match source-address 0.0.0.0/0
```

```
set security nat source rule-set SNAT_RuleSet rule SNAT_Rule then source-nat interface
commit
```

Example: Configure Juniper Sky ATP for vSRX

IN THIS SECTION

This example shows how to configure Juniper Sky™ Advanced Threat Prevention (Juniper Sky ATP) on a vSRX instance that is deployed in a virtual private cloud (VPC).

Before You Begin

Ensure that you have installed and launched a vSRX instance in a VPC.

Overview

You can use Juniper Sky ATP, a cloud-based solution, along with vSRX to protect all hosts in your network against evolving security threats.

Juniper Sky ATP Configuration

IN THIS SECTION

Procedure

Step-by-Step Procedure

To configure Juniper Sky ATP on a vSRX instance:

1. Log in to the vSRX instance using SSH and start the CLI.

```
root@% cli
root@>
```

2. Enter configuration mode.

```
root@> configure
[edit]
root@#
```

3. Set up the correct data interface for the active advanced antimalware (AAMW) service instead of using the default fxp0 interface.

```
root@# set services advanced-anti-malware connection source-interface ge-0/0/0.0
```

4. Configure NAT.

```
root@# set security nat source rule-set rs1 from zone trust
root@# set security nat source rule-set rs1 to zone untrust
root@# set security nat source rule-set rs1 rule r1 match source-address 0.0.0.0/0
```

```
root@# set security nat source rule-set rs1 rule r1 match destination-address 0.0.0.0/0
root@# set security nat source rule-set rs1 rule r1 then source-nat interface
```

5. Set up virtual routing instance for the correct data interface for AAMW service.

```
root@# set routing-instances vsrx-vr1 instance-type virtual-router
root@# set routing-instances vsrx-vr1 routing-options static route 0.0.0.0/0 next-hop 10.4.1.1
root@# set routing-instances vsrx-vr1 interface ge-0/0/0.0
root@# set routing-instances vsrx-vr1 interface ge-0/0/1.0
```

6. Verify the configuration.

```
root@# commit check
configuration check succeeds
```

7. Commit the configuration to activate it on the vSRX instance.

```
root@# commit
commit complete
```

8. Optionally, you can verify the configuration by running the following show commands in the configuration mode:

   - show services advanced-anti-malware connection | display set
   - show security nat | display set
   - show routing-instances vsrx-vr1 | display set

RELATED DOCUMENTATION

Juniper Sky Advanced Threat Prevention Administration Guide

5

CHAPTER

Monitoring and Troubleshooting

Monitoring

IN THIS SECTION

Monitoring vSRX Instances Using SNMP

This topic provides details on how you can monitor your vSRX instances using SNMP and GCP monitoring features.

Monitoring helps in maintaining the reliability, availability, and performance of your vSRX instances and your GCP solution. You should collect monitoring data from all your GCP solution so that you can easily debug any multi-point failure.

You can monitor your vSRX instance details such as health and storage at instance level, using SNMP monitoring.

For details on SNMP monitoring, refer the SNMP MIB information in the MIB Explorer at: https://apps.juniper.net/mib-explorer/.

You can also find all the applicable SNMP OIDs from the Juniper MIB from the vSRX CLI, using the **show snmp mib walk 1.3.6.1.4.1.2636** command.

Some examples of useful OID's for monitoring system health are:

```
jnxOperatingCPU.1.1.0.0
jnxOperating5MinAvgCPU.1.1.0.0
jnxFwddMicroKernelCPUUsage.0
jnxFwddRtThreadsCPUUsage.0
jnxHrStoragePercentUsed.1
jnxJsNodeCurrentTotalSession.0
jnxJsNodeMaxTotalSession.0
jnxJsNodeSessionCreationPerSecond.0
```

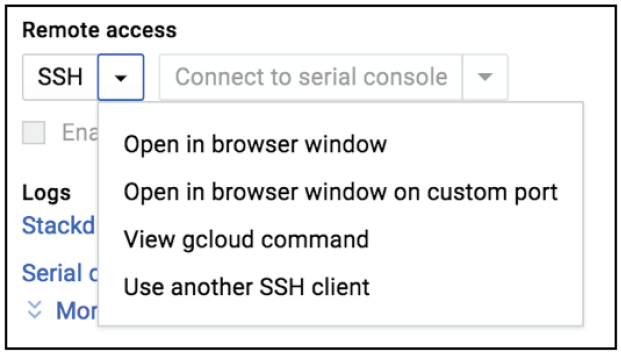
NOTE: For monitoring storage capacity on the vSRX instance you can use SNMP monitoring. Using SNMP monitoring, you can be notified for any vSRX instance storage that is impacted. The storage related OID indicates the storage percentage, which is used to detect the storage capacity.

For best practices for enabling SNMP monitoring in Junos, see https://www.juniper.net/documentation/en_US/junos/topics/ task/configuration/snmp-best-practices-basic-config.html.

Monitoring vSRX Instance Using GCP Features

Google Cloud Engine (GCE) provides multiple methods to remotely access the vSRX VMs. For enabling monitoring, GCE adds the SSH public key to the VM. On vSRX we need to specifically define the SSH key to be used for the instance at instance creation time.

Figure 19: Defining SSH Key for vSRX VMs



For vSRX to use the console port, the console parameter should be set as **console=ttyS0,38400n8**.

Finding the Software Serial Number for vSRX

You need the software serial number to open a support case or to renew a vSRX license.

The serial number is a unique 14-digit number that Juniper Networks uses to identify your particular software installation. You can find the software serial number in the Software Serial Number Certificate attached to the e-mail that was sent when you ordered your Juniper Networks software or license. You can also use the show system license command to find the software serial number.

Use the **show system license** command to find the vSRX software serial number.

```
vsrx> show system license
```

```
License usage:
                                Licenses     Licenses    Licenses    Expiry
  Feature name                       used    installed      needed
  Virtual Appliance                     1            1           0    58 days

Licenses installed:
  License identifier: E420588955
  License version: 4
  Software Serial Number: 20150625
  Customer ID: vSRX-JuniperEval
  Features:
    Virtual Appliance - Virtual Appliance
      count-down, Original validity: 60 days

  License identifier: JUNOS657051
  License version: 4
  Software Serial Number: 9XXXXAXXXXXXX9
  Customer ID: MyCompany
  Features:
    Virtual Appliance - Virtual Appliance
      permanent
```

For more information, see Licenses for vSRX